

09/578,474
YO999 - 486

2

12 identification data is known only to said third party.

1 2. (Amended) A method of performing electronic commerce without a candidate customer
2 being forced to disclose private data together with an identity of the candidate customer, to a
3 business entity requiring said private data, said method comprising:
4 establishing an intermediary relationship with a third party between the candidate
5 customer and the business entity;
6 providing a proprietary item to said customer such that the customer can be identified as a
7 legitimate owner of the item without revealing the identity of said customer; and
8 performing electronic commerce between said customer and said business entity through
9 said third party, utilizing said proprietary item, such that an identity of said customer is kept from
10 said business entity party,
11 wherein said business entity is provided with information identifying said customer only
12 as a transactional party in said electronic business transaction, and
13 wherein said providing an intermediary relationship by said third party comprises
14 replacing an identification data about said first party with an identifier whose linkage to said
15 identification data is known only to said third party.

B² 6. (Amended) The method according to claim 5, wherein said portable device P(C) generates
numbers $S(C,n)$, where n is an integer belonging to a set $\{1, 2, \dots, N\}$, and
wherein for at least one of a new business entity and another partner of the customer, a
new number n is chosen for all further transactions between the customer and said at least one of
said new business unit and said another partner.

B³ 11. (Amended) The method according to claim 2, wherein, before establishing an intermediary
relationship, the customer accesses one or more verifiers V_j , and
wherein the customer identifies itself to each verifier V_j using a number $S(C)$ associated
with the proprietary item, and requests V_j to send $S(C)$ to the business entity, together with data
verified by V_j .

12. (Amended) The method according to claim 11, wherein communication to the business

09/578,474
YO999 - 486

3

entity is performed by appending to the number S(C) a non-identity data relevant to the customer encrypted using $pu1(I)$.

13. (Amended) The method according to claim 11, wherein a link between the third party and the business entity is provided by the third party posting one or more completed application on a dedicated world-wide-web (WWW) page after replacing customer identification data with a number N(T,C, I) which allows the business entity, but no other party, to recognize this number as a number associated with the business entity.

14. (Amended) The method according to claim 2, wherein a payment between a business entity and a third party is documented by a paying party by attaching a tagging number to the payment, said tagging number being communicated to a bank of the paying party, and accompanies a transaction order to the bank of the payee, and

wherein the paying bank authorizes a money transfer in exchange for a tag coded using a private key of the payee's bank.

16. (Amended) The method according to claim 15, wherein, when a transaction request is submitted, the customer addresses the transaction request to the third party, after selectively consulting with one or more verifiers Vj.

24. (Amended) A method of selecting a purveyor of goods or services in a confidential manner over a network, comprising:

sending, by a customer to a third party, an application and software for encrypting the application using a public key $pu1(I)$,

wherein said application is taken electronically from a business entity,

wherein a public signature scheme of said business entity is $(Pr1(I), pu1(I))$, software

allowing the customer to compute a public signature scheme $(Pr2(I,C), pu2(I,C))$, and

wherein said business entity is provided with information identifying said customer only as a transactional party in said electronic business transaction, and

wherein said third party replaces an identification data about said customer with an identifier whose linkage to said identification data is known only to said third party.

09/578,474
YO999 - 486

4

1 34. (Amended) A system for conducting business electronically between a first party and a
2 second party, comprising:
3 means for providing to a third party an identity of the first party but no
4 privacy-compromising information regarding a proposed electronic business transaction between
5 the first party and second party; and
6 means for conducting the electronic business transaction between said first party and
7 second party through the third party such that said identity of said first party is kept from the
8 second party,
9 wherein said second party is provided with information identifying said first party only as
10 a transactional party in said electronic business transaction, and
11 wherein said third party replaces an identification data about said first party with an
12 identifier whose linkage to said identification data is known only to said third party.

16 35. (Amended) A signal-bearing medium tangibly embodying a program of machine-readable
2 instructions executable by a digital processing apparatus to perform a method for conducting
3 business electronically between a first party and a second party, said method comprising:
4 providing to a third party an identity of the first party but no privacy-compromising
5 information regarding a proposed electronic business transaction between the first and second
6 parties; and
7 conducting the electronic business transaction between said first and second parties
8 through the third party such that said identity of said first party is kept from the second party,
9 wherein said second party is provided with information identifying said first party only as
10 a transactional party in said electronic business transaction, and
11 wherein said third party replaces an identification data about said first party with an
12 identifier whose linkage to said identification data is known only to said third party.

1 36. (Amended) A system for performing electronic commerce without a candidate customer
2 being forced to disclose private data together with an identity of the candidate customer to a
3 business entity requiring said private data, said system comprising:
4 means for establishing an intermediary relationship with a third party between the

09/578,474
YO999 - 486

5

candidate customer and the business entity;

a proprietary item provided to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer; and

means for performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that an identity of said customer is kept from said business entity party,

wherein said business entity is provided with information identifying said candidate customer only as a transactional party in said electronic commerce, and

wherein said third party replaces an identification data about said customer with an identifier whose linkage to said identification data is known only to said third party.

37. (Amended) A signal-bearing medium tangibly embodying a program of machine- readable instructions executable by a digital processing apparatus to perform a method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer; and

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that an identity of said customer is kept from said business entity,

wherein said business entity is provided with information identifying said customer only as a transactional party in said electronic commerce, and

wherein said third party replaces an identification data about said customer with an identifier whose linkage to said identification data is known only to said third party.

38. (Amended) A method of conducting business electronically between a first party and a second party, comprising:

providing an intermediary relationship with a third party who knows an identity of the

09/578,474
YO999 - 486

6

first party but no privacy-compromising information regarding a proposed electronic business transaction between the first party and the second party; and

conducting the electronic business transaction between said first party and said second party through the third party such that said identity of said first party is kept from the second party, but second party can obtain confidential data about first party that do not compromise the identity of said first party,

wherein said third party replaces an identification data about said first party with an identifier whose linkage to said identification data is known only to said third party.

39. (Amended) A method of conducting business electronically between a first party and a second party, comprising:

providing an intermediary relationship with a third party who knows an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first and second parties, said third party enabling communications between the first and second party and having access to the identity but not to the content or the nature of the transaction; and

conducting the electronic business transaction between said first and second parties so that the identity of said first party is not available to the second party,

wherein said second party receives confidential data about said first party unrelated to the identity of said first party, and

wherein said third party replaces an identification data about said first party with an identifier whose linkage to said identification data is known only to said third party.

41. (Amended) A method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer, to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing an identity of said customer; and

performing electronic commerce between said customer and said business entity through

09/578,474
YO999 - 486

7

9 said third party, utilizing said proprietary item, such that the identity of said customer is unknown
10 to said business entity,

67 11 wherein said third party can recognize, without having access to an identity, each
12 customer to conduct business over an extended period of time and in repeated interactions, and
13 accumulate all data needed to service the customer, to conglomerate such data to provide a
14 customer history or subject the data to data mining technologies, and

15 wherein said third party replaces an identification data about said customer with an
16 identifier whose linkage to said identification data is known only to said third party.
